Contents

[hide]

目的

- 了解電子郵件運作
- 使用替代制度，以選擇一個郵件服務器
- 執行基本配置郵件服務器
- 配置procmail
- 配置dovecot加密和不加密的議定
- 除錯電子郵件服務

電子郵件服務

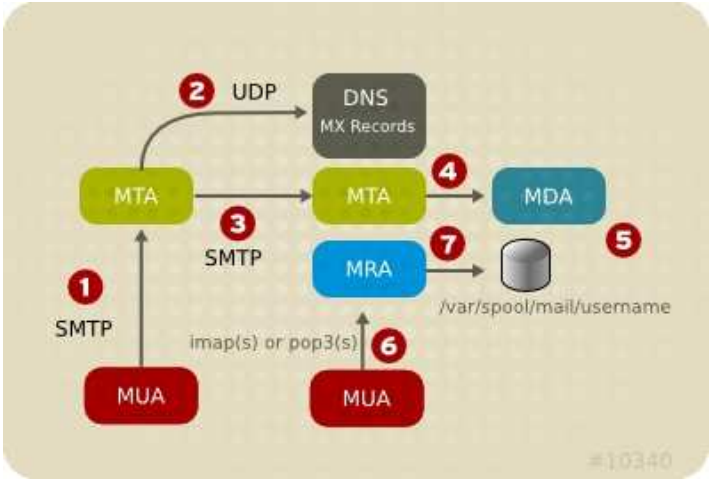
Email 系統組成的元件

- Email 系統組成的元件：

1. MUA(Mail User Agent):收發郵件的程式，ex. outlook, mutt, thunderbird
2. MTA(Mail Transfer Agent):傳遞轉交信件的程式, ex. sendmail, postfix
3. MDA(Mail Delivery Agent):儲存處理信件的程式, procmailrc, mailscanner
4. MAA(Mail Access Agent):存取訊息的程式, ex. Dovecot, Cyrus IMAP

Email簡介

- 必要的 Email 操作流程



- 流程說明：

1. 郵件 client 端對 mta 發出 smtp 寄信動作
2. mta 先查詢 dns 郵件收信人的 ip 位址
3. mta 依據查詢到的 ip 發信給對方的 mta 機器
4. 對方的 mta 機器依據 mda 規則將信件寫入檔案 /var/spool/mail/ 目錄

5. mua 對 mra 發出 pop3 或 imap 收件需求
6. mra 去系統的 /var/spool/mail 目錄找到資料

- 只要主機名稱對應到 IP 就可以架設 mail server 。
- DNS 的 MX Record 用途是當主要的 mail server 掛掉時，信件不會直接退回，而是跑到下一個 MX 設定的主機去，並且暫存在該處，等到主要的 mail server 復活後將信件傳送到目的地。

Simple Mail Transport Protocol

- RFC-standard protocol for talking to MTA's

1. Almost always uses TCP port 25
2. Extended SMTP (ESMTP) provides enhanced features for MTA's
3. An MTA often uses Local Mail Transport Protocol (LMTP) to talk to itself

- 底下的操作和下面者行指令雷同(會自動產生)

1. mail -vs 'test' test@stationX.example.com
2. test
3. .

- 使用 telnet troubleshoot SMTP connections ，這裡使用 station1.example.com 的 smtp 當示範。

```
[root@station1 ~]# telnet station1.example.com 25
Trying 172.24.0.1...
Connected to station1.example.com (172.24.0.1).
Escape character is '^]'.
220 station1.example.com ESMTP Sendmail 8.13.8/8.13.8; Sun, 9 Nov 2008 14:00:38 +0800
HELO staion1.example.com
250 station1.example.com Hello station1.example.com [172.24.0.1], pleased to meet you
MAIL From: test@station1.example.com
250 2.1.0 test@station1.example.com... Sender ok
RCPT To:root@station1.example.com
250 2.1.5 root@station1.example.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
test
.
250 2.0.0 mA960cOn032745 Message accepted for delivery
QUIT
221 2.0.0 station1.example.com closing connection
Connection closed by foreign host.
```

SMTP 防火牆

- Network layer with Netfilter stateful inspection

1. 內部(Inbound) 和外部(outbound)都是使用 TCP port 25

- 應用層中繼(relay)保護

1. Internal MTA to which users connect for sending and receiving
2. DMZ-based outgoing smart host which relays mail from the internal MTA
3. DMZ-based inbound mail hub which relays mail to the internal MTA
4. 過濾規則 within the DMZ MTA's or integrated applications (e.g., Spamassassin)

Mail Transport Agents

- CentOS Linux 包含三種 MTA's (郵件傳輸伺服器)

1. Sendmail (default MTA), Postfix, and Exim

- Common features

1. Support virtual hosting
2. Provide automatic retry for failed delivery and other error conditions
3. Interoperable with Spamassassin

- 預設的存取控制

1. Sendmail and Postfix have no setuid components
2. Listen on loopback only
3. 預設 Relaying 是關閉的

- SPAM

1. http://spam.abuse.org
2. spamassassin http://spamassassin.apache.org/

Sendmail 電子郵件設定

伺服器資訊：Sendmail

- 型態: System V-managed service
- 套件: sendmail, sendmail-cf, sendmail-doc
- 服務: /usr/sbin/sendmail
- 啟動程序: /etc/init.d/sendmail
- Port: 25 (smtp)
- 設定檔: /etc/mail/sendmail.mc, /etc/aliases, and others
- 相關的套件: procmail (MDA), spamassassin, tcp_wrappers, sendmail-doc
- 基本上包含這幾個 RPM 套件

```
[root@station1 ~]# rpm -qa | grep sendmail
sendmail-8.13.8-2.el5
sendmail-cf-8.13.8-2.el5
[root@station1 ~]# rpm -qa | grep m4
m4-1.4.5-3.el5.1
```

- sendmail 支援 TCP Wrappers 存取控制

```
[root@station1 ~]# ldd /usr/sbin/sendmail | grep libwrap
        libwrap.so.0 => /usr/lib/libwrap.so.0 (0x00f06000)
```

初始 Sendmail Configuration

- CentOS 使用 m4 巨集語言

1. 使用 dnl 加上空白解釋每一行 within an m4 巨集檔案

- service sendmail restart 這個指令是使用 /etc/mail/Makefile 檔案，並執行下列三個動作

1. 轉換 /etc/mail/sendmail.mc(m4巨集檔) 轉成 /etc/mail/sendmail.cf
2. 重新設定變數為 flat-file databases
3. 建立比較時間戳記; 觸摸一各檔案並強迫 rebuild/rehash

- sendmail-cf 預設並沒有安裝，這個啟動程序(service sendmail restart)，如果缺少 sendmail-cf 的安裝不會建立檔案。所以說如果不動會請安裝：

```
# yum install sendmail-cf -y
```

- 所以講了這麼多，就是只要執行下列指令就可以啟動

```
#  service sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]
```

進入(Incoming)信件的 Sendmail 設定

- 請先執行 setup 設定好你的電腦的 hostname 、IP及DNS，確定都設定正確。

```
$ setup
```

- 請先確定你的 dns 正解正確，最好連 MX record都有設定。

```
# host station1.example.com
station1.example.com has address 172.24.0.1
station1.example.com mail is handled by 10 station1.example.com.
```

- 修改 /etc/mail/sendmail.mc to listen on all interfaces(設定為 0.0.0.0)大約在 116行附近。
    - dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

```
[root@station1 ~]# vi /etc/mail/sendmail.mc
DAEMON_OPTIONS(`Port=smtp,Addr=0.0.0.0, Name=MTA')dnl
```

- 加入到 /etc/mail/local-host-names 每個 hostname by which the server may be referred

```
# local-host-names - include all aliases for your machine here.
# 這裡設定包含這台主機有可能收到信件的名稱，sendmail會接收這裡所設的網域郵件
station1.example.com
```

- 修改存取控制(ACL)包含 TCP Wrapper and iptables

1. Update /etc/hosts.{allow,deny}
2. Add an Netfilter rule to allow SMTP traffic

- 在 hosts.allow and hosts.deny 的設定，及設定後log的回應(可以不用設定,如果你不想擋住其他主機的話)

```
# vim /etc/hosts.allow
sendmail:172.24.0.0/255.255.0.0:allow
sendmail:ALL:deny

# 可以觀看紀錄 tail /var/log/maillog  他的 reject 狀況如下
Oct 11 13:58:07 linux sendmail[10440]: n9B5w7Bc010440:
tcpwrappers (unknown, 115.165.192.55) rejection
(節錄部份skip.....)
```

- Restart sendmail 並驗證服務

```
[root@station1 mail]# service sendmail restart
Shutting down sm-client:                                   [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Starting sendmail:                                         [  OK  ]
Starting sm-client:                                        [  OK  ]

# 你需要確認 listen 的位址在 0.0.0.0 而不是 127.0.0.1
[root@station1 mail]# netstat -tnlup | grep sendmail
tcp        0      0 0.0.0.0:25                  0.0.0.0:*
              LISTEN      3331/sendmail: acce
```

- 看一下目前的 sendmail 站台設定有無問題，有問題請修改 /etc/sysconfig/network 及 /etc/hosts 的內容

```
[[root@station1 mail]# sendmail -d0 < /dev/null
Version 8.13.8
 Compiled with: DNSMAP HESIOD HES_GETMAILHOST LDAPMAP LOG MAP_REGEX
                MATCHGECOS MILTER MIME7TO8 MIME8TO7 NAMED_BIND NETINET NETINET6
                NETUNIX NEWDB NIS PIPELINING SASLv2 SCANF SOCKETMAP STARTTLS
                TCPWRAPPERS USERDB USE_LDAP_INIT

============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = station1
  (canonical domain name) $j = station1.example.com
         (subdomain name) $m = example.com
              (node name) $k = station1.example.com
```

```
==========================================================

Recipient names must be specified
```

- 從另外一台主機寄信作測試，底下是從 server1.example.com 寄出

```
[root@server1 ~]# mail root@station1.example.com
Subject: test to station1
test mail to station1
.
Cc:
# 如果為了方便,也可以直接輸入,底下的指令
# echo 'test' | mail -s "$(date +%Y%m%d%s)" root@station1.example.com
```

- 寄完可以查看 /var/log/maillog 會告訴你相關的寄出郵件訊息.
- 從 root@station1.example.com 主機會收到來自於 root@server1.exmaple.com 的信件

```
You have new mail in /var/spool/mail/root
[root@station1 ~]# mail
Message 15:
From root@server1.example.com  Sun Nov  9 13:56:56 2008
Date: Sun, 9 Nov 2008 13:56:58 +0800
From: root <root@server1.example.com>
To: root@station1.example.com
Subject: test to station1

test mail to station1
```

- 一樣接收端的 /var/log/maillog 也會有相關的紀錄存在.
- 也可以直接看 /var/spool/mail 內的內容size變化,就知道有沒有信件近來

寄出的信件(Outgoing) Sendmail 設定

- Red Hat 提供預設的 /etc/mail/submit.cf

1. 罕有需要修改
2. 啟動 sendmail to act as a client MSP(mail-submission program)

- To 偽裝一個 Domain 來替代一個站台
    - 取消註解這行 in /etc/mail/sendmail.mc

```
EXPOSED_USER(`root')dnl
FEATURE(masquerade_envelope)dnl
MASQUERADE_AS(`example.com')dnl
FEATURE(masquerade_entire_domain)dnl
```

- These options work in 結合 with 向外去的 address rewriting

```
dnl MASQUERADE_AS(`station1.example.com')dnl
```

- ref:http://docs.sun.com/app/docs/doc/816-4555/mailrefer-106?l=zh_tw&a=view
- ref:http://www.harker.com/sendmail/submit.html

進來的信件 Sendmail Aliases

- 本地端的代名: /etc/aliases
- 程式必須被聯結到 /etc/smrsh 為了這個 (Sendmail Restricted Shell)-->smrsh

```
fakename: realname
a-list:   fakename, otheruser
helpdesk: | mail2ticket
```

- 虛擬的代名: /etc/mail/virtusertable

```
admin@123.com       shopper
admin@xyz.org       jdj
pageme@he.net       lmiwtc@pg.com
@cba.com            cba@aol.com
@dom1.org           %1@dom2.org
```

- 把 root 的信轉寄到 admin

```
[root@station1 mail]# vi /etc/aliases
root:           admin
[root@station1 mail]# newaliases
/etc/aliases: 77 aliases, longest 10 bytes, 774 bytes total
```

出站的地址重寫

- 信件寄出，改寫檔頭，然後轉到內部指定的信箱(SMTP服務限定)
- 增加底下這3行在 /etc/mail/sendmail.mc 內，在 MAILER(smtp)dnl 這行之前。

```
FEATURE(genericstable)dnl
FEATURE(`always_add_domain')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/local-host-names')dnl
```

- 建立 /etc/mail/genericstable 這檔案

```
paul@example.com    paul@otherexample.com
david@example.com   david.lastname@example.com
```

- 網域名稱(Domains)必須在 /etc/mail/local-host-names 內有被聆聽。
- 位址重寫只會發生在 SMTP 不是在 LMTP

Sendmail SMTP 限制

- 拒絕符合描述條件的郵件存取
- 啟動 Enable in /etc/mail/sendmail.mc 使用底下這行

1. FEATURE(`blacklist_recipients')dnl

- 並且在 /etc/mail/access 設定限制

```
From:90trialspammer@aol.com     REJECT
Connect:spamRus.net             REJECT
Connect:204.168.23              REJECT
Connect:10.3                    OK
From:virtualdomain1.com         RELAY
To:user@dom9.com                ERROR:550 mail discarded
To:nobody@                      ERROR:550 bad name
```

- 使用 tag 指示是否 blacklisting 生效於送件者, 接收者, or MTA
- 不使用 tag 條目是聲明不贊成 Sendmail
- 這各/etc/mail/access 資料庫檔案，能夠對於非法的使用者回絕email，可以針對 individual users , entire domain, 及 entire IP subnet. 有幾種方式的語法可以針對這資料庫作描述。

1. REJECT
2. OK
3. RELAY
4. DISCARD
5. ERROR:550

- 詳細請見 http://www.sendmail.org/m4/anti_spam.html 說明

Sendmail 操作

- /etc/mail/local-host-names
    - 必須含有 Server's name and aliases

- mail -v user
  - 觀看 SMTP 本地端的交換狀況
- mailq and mailq -Ac
  - 觀看訊息佇列及未來將傳送的信件
- sendmail -q
  - 報告在email佇列中的處理程序
- tail -f /var/log/maillog
  - 即時觀看log檔案

使用 **alternatives** 指令切換 **MTAs(**郵件服務系統**)**

- 關於 the alternatives system

1. displays or configures the preferred MTA and associated man pages based on a generic name
2. 一般的名稱都被連結到 /etc/alternatives/ 目錄內
3. 只有這些連結被修改 in /etc/alternatives/

- 切換 MTA's

1. 停止目前的 MTA and 並且關避開機啟動
2. 切換設定檔 alternatives --config mta and make a selection
3. Start the new MTA and enable boot-time startup

- Graphical interface: system-switch-mail-gnome package
- 切換 sendmail to postfix
- 關閉 sendmail and turn off boot-time startup

```
[root@linux ~]# /etc/init.d/sendmail stop
[root@linux ~]# chkconfig sendmail off
```

- 文字型的切換 mail system

```
[root@linux ~]# alternatives --config mta

有 2 程式提供 'mta'。

  選擇         指令
-----------------------------------------------
*+ 1           /usr/sbin/sendmail.sendmail
   2           /usr/sbin/sendmail.postfix

請輸入以保留目前的選擇[+]，或輸入選擇號碼:2
```

- 打開 postfix 並且預設開機啟動

```
[root@linux ~]# /etc/init.d/postfix restart
[root@linux ~]# chkconfig postfix on
```

Postfix 電子郵件服務

Service Profile: Postfix

- Type: SystemV-managed service
- Package: postfix
- Daemons: /usr/libexec/postfix/master and others
- Script: /etc/init.d/postfix
- Port: 25 (smtp)

- Port: 25 (smtp)
- Configuration: /etc/postfix/main.cf and others
- Related: procmail

```
[root@linux ~]# yum install postfix -y
```

初始 Postfix 設定檔

- /etc/postfix/main.cf

1. Well-commented key=value pairs, evaluated in the order in which they appear
2. White space at beginning of line is continuation character
3. Keys 會使用後來才設定的變數 key=value pairs

```
key1=value1
key2=$key1, value2
```

- postconf

1. 顯使預設的設定值: postconf -d
2. 顯示目前為預設的設定: postconf -n
3. 單獨修改某各設定 in main.cf: postconf -e key=value
4. Show supported map types: postconf -m

可以接收信件Incoming的Postfix設定

- 設定你的email前請先確定你的 hostname and DNS正解及MX紀錄(最少要有A紀錄)。

```
[root@linux ~]# hostname
linux.jangmt.com
[root@linux ~]# host linux.jangmt.com
linux.jangmt.com has address 140.117.69.184
```

- 修改 /etc/postfix/main.cf

1. Listen on all interfaces

```
inet_interfaces = all
```

- 伺服器要接收的郵件位址，底下為預設(相當於 sendmail的 /etc/mail/local-host-names檔案用途)

```
mydestination = $myhostname, localhost.$mydomain,
                      localhost, $mydomain
```

- 如果你的 hostname 有設定好可以直接用上面那一行，如果沒有請手動修改為你的主機名稱

```
mydestination = linux.jangmt.com, loclhost
```

- 增加 Netfilter 規則，允許 SMTP traffic 通過
- 重新啟動 postfix

```
[root@linux ~]# /etc/init.d/postfix restart
```

- 驗證 socket

```
[root@linux ~]# netstat -tnulp | grep 25
tcp        0      0 0.0.0.0:25                  0.0.0.0:*
       LISTEN      11815/master
```

- 從另一台主機寄出信件

```
[root@antai ~]# echo 'test' | mail -v -s "$(date +%Y%m%d%s)" mtchang@linux.jangmt.com
mtchang@linux.jangmt.com... Connecting to [127.0.0.1] via relay...
220 antai.jangmt.com ESMTP Sendmail 8.13.8/8.13.8; Sun, 11 Oct 2009 23:13:28 +0800
>>> EHLO antai.jangmt.com
250-antai.jangmt.com Hello antai.jangmt.com [127.0.0.1], pleased to meet you
250-ENHANCEDSTATUSCODES
```

```
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
>>> MAIL From:<root@antai.jangmt.com> SIZE=63 AUTH=root@antai.jangmt.com
250 2.1.0 <root@antai.jangmt.com>... Sender ok
>>> RCPT To:<mtchang@linux.jangmt.com>
>>> DATA
250 2.1.5 <mtchang@linux.jangmt.com>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 n9BFDSku014497 Message accepted for delivery
mtchang@linux.jangmt.com... Sent (n9BFDSku014497 Message accepted for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 antai.jangmt.com closing connection
```

- 到收件端收信，應該可以收到信件就算成功。

Outgoing Postfix Configuration

- Red Hat provides a default /etc/postfix/main.cf

1. Enables Postfix to act as a client MSP
2. No further configuration needed for single host
3. Postfix automatically resolves local hostname and domain

- To masquerade as a domain

```
myorigin = $mydomain
masquerade_exceptions = root
```

Inbound Postfix Aliases

- Local aliases: /etc/aliases as in Sendmail
- Virtual aliases

1. Enable in main.cf

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

1. Define in /etc/postfix/virtual using the same format as Sendmail
2. Rehash the file: postmap /etc/postfix/virtual

Outbound Address Rewriting

- Enable in /etc/postfix/main.cf
- smtp in the key name indicates SMTP only (not LMTP)

```
smtp_generic_maps = hash:/etc/postfix/generic
```

- Define in /etc/postfix/generic

```
paul@example.com    paul@otherexample.com
david@example.com   david.lastname@example.com
```

- Rehash the file: postmap /etc/postfix/generic

Postfix SMTP 限制

- 建立 /etc/postfix/access
- untagged version of Sendmail access file

- untagged version of Sendmail access file
- rehash using postmap /etc/postfix/access

- Edit main.cf

```
smtpd_TAG_restrictions = check_TAG_access hash:/etc/postfix/access, ...
```

- TAG is one of sender, recipient, or client
- Example:

```
smtpd_recipient_restrictions =
         check_recipient_access hash:/etc/postfix/access,
         permit_mynetworks, reject_unauth_destination
```

- 更多詳細 man 5 postconf

mail Relay

- 允許誰可以對此台 mail server 作 smtp 寄件的動作

```
[root@station1 ~]# vim main.cf
# Specify "mynetworks_style = host" when Postfix should "trust"
# only the local machine.
#
#mynetworks_style = class
# 預設為本地的mask設定的subnet可以發信
mynetworks_style = subnet
#mynetworks_style = host

# You can also specify the absolute pathname of a pattern file instead
# of listing the patterns here. Specify type:table for table-based lookups
# (the value on the table right-hand side is not used).
# 允許 192.168.3.0/24 這個 class C網段及 127.0.0.1 本機可以 smtp 發信
mynetworks = 192.168.3.0/24, 127.0.0.1
#mynetworks = 168.100.189.0/28, 127.0.0.0/8
#mynetworks = $config_directory/mynetworks
#mynetworks = hash:/etc/postfix/network_table
```

Postfix 操作

- main.cf 設定

1. Server names: mydestination 必須包含 server's name and aliases
2. Listening 介面: inet_interfaces = all
3. 收集所有的mail: always_bcc = address

- 觀看 SMTP exchange: mail -v user@domain.tld
- 觀看延遲的訊息: postqueue -p
- 更新延遲的訊息: postqueue -f
- 即時觀看 log: tail -f /var/log/maillog

- always_bcc example:

```
always_bcc=mtchang@linux.jangmt.com
```

- 這樣只要信件透過這台主機傳送，全部會被以BCC方式傳遞到後面的email address

Procmail

Procmail, 信件轉寄的代理人

- 不同的使用包括:

1. 排序接收不同的Email到檔案或資料夾

2. 預先處理信件 email
3. 啟動一個事件或是程式，當email抵達時
4. 自動轉寄信件到他人

- 啟動 Procmail 代理人

1. Sendmail: enabled by default
2. Postfix: 修改 /etc/postfix/main.cf
    1. 加入 mailbox_command = /usr/bin/procmail

Procmail 及存取控制

- 初始化控制

1. SELinux 的政策限制了mail工具到特定的目錄
2. Procmail 執行時期的權限為 nobody
3. Procmail 的擁有者是 mail group 群組
4. /var/spool/mail 目錄只能夠被 root and the mail group 寫入

- 需要變更: change the procmail binary to run setgid

```
chmod g+s $(which procmail)
```

Procmail 設定檔

- 設定檔會依序被下列的設定檔讀取處理
- 全域procmailrc設定:

1. /etc/procmailrc
2. LOGFILE=/var/log/procmail.log

- 個人procmailrc設定:

1. ~/.procmailrc (個人)
2. LOGFILE=$HOME/.procmail_log

- 原理 within a configuration file

1. Directives: VERBOSE=yes yes/on=啟用詳細訊息; no/off=關閉詳細訊息
2. Variables: LOGFILE=/var/spool/mail/procmail.log 指定 error message 和 diagnostic message 寫入的檔案

- 基本原則：以正規表示法(Regular Expression)透過egrep分析郵件內容 (預設不區分大小寫)

1. 每一個規則的描述開始從 ":0" 這裡開始
2. 零或更多的符合的行使用 regular expressions 比對
3. 可以有一個或多個動作行

Sample Procmail 方法

- man procmailrc 的說明內容節錄

方法

```
A line starting with ':' marks the beginning of a recipe.  It  has
the following format:

       :0 [flags] [ : [locallockfile] ]
       <zero or more conditions (one per line)>
       <exactly one action line>
```

條件的判斷起始於 `*', 每個在後面的字元是透過 egrep 指令過濾條件逐步的比對。
這正規表示式相容於使用 egrep(1) 擴充正規表示式

Flags 的用途如下所列：

H 只 Egrep 郵件檔頭(預設值).

B 只 Egrep 郵件內文.

h Feed the header to the pipe, file or mail destination (default).

b Feed the body to the pipe, file or mail destination (default).

f Consider the pipe as a filter.

c Generate a carbon copy of this mail. This only makes sense on delivering recipes. The only non-delivering recipe this flag has an effect on is on a nesting block, in order to generate a carbon copy this will clone the running procmail process (lockfiles will not be inherited), whereby the clone will proceed as usual and the parent will jump across the block.

Local lockfile

If you put a second (trailing) ':' on the first recipe line, then procmail will use a locallockfile (for this recipe only). You can optionally specify the locallockfile to use; if you don't however, procmail will use the destination filename (or the filename following the first '>>') and will append $LOCKEXT to it.

Recipe action line

The action line can start with the following characters:

! Forwards to all the specified mail addresses.

| Starts the specified program, possibly in $SHELL if any of the characters $SHELLMETAS are spotted. You can optionally prepend this pipe symbol with variable=, which will cause stdout of the program to be captured in the environment variable (procmail will not terminate processing the rcfile at this point). If you specify just this pipe symbol, without any program, then procmail will pipe the mail to stdout.

{ Followed by at least one space, tab or newline will mark the start of a nesting block. Everything up till the next closing brace will depend on the conditions specified for this recipe. Unlimited nesting is permitted. The closing brace exists merely to delimit the block, it will not cause procmail to terminate in any way. If the end of a block is reached processing will continue as usual after the block. On a nesting block, the flags `H' and `B' only affect the conditions leading up to the block, the flags `h' and `b' have no effect whatsoever.

Environment variable defaults

LOGNAME, HOME and SHELL	Your (the recipient's) defaults
PATH	$HOME/bin:/usr/local/bin:/usr/bin:/bin (Except during the processing of an /etc/procmailrc file, when it will be set to `/usr/local/bin:/usr/bin:/bin'.)
SHELLMETAS	&|<>~;?*[
SHELLFLAGS	-c
ORGMAIL	/var/mail/$LOGNAME (Unless -m has been specified, in which case it is unset)
MAILDIR	$HOME (Unless the name of the first successfully opened rcfile starts with `./' or if -m has been specified, in which case it defaults to `.')
DEFAULT	$ORGMAIL
MSGPREFIX	msg.
SENDMAIL	/usr/sbin/sendmail
SENDMAILFLAGS	-oi
HOST	The current hostname
COMSAT	no

COMSAT no

Environment

Before you get lost in the multitude of environment variables, keep in mind that all of them have reasonable defaults.

MAILDIR Current directory while procmail is executing (that means that all paths are relative to $MAILDIR).

DEFAULT Default mailbox file (if not told otherwise, procmail will dump mail in this mailbox). Procmail will automatically use $DEFAULT$LOCKEXT as lockfile prior to writing to this mailbox. You do not need to set this variable, since it already points to the standard system mailbox.

LOGFILE This file will also contain any error or diagnostic messages from procmail (normally none :-) or any other programs started by procmail. If this file is not specified, any diagnostics or error messages will be mailed back to the sender. See also LOGABSTRACT.

VERBOSE You can turn on extended diagnostics by setting this variable to `yes' or `on', to turn it off again set it to `no' or `off'.

LOGABSTRACT Just before procmail exits it logs an abstract of the delivered message in $LOGFILE showing the `From ' and `Subject:' fields of the header, what folder it finally went to and how long (in bytes) the message was. By setting this variable to `no', generation of this abstract is suppressed. If you set it to `all', procmail will log an abstract for every successful delivering recipe it processes.

LOG Anything assigned to this variable will be appended to $LOGFILE.

TIMEOUT Number of seconds that have to have passed before procmail decides that some child it started must be hanging. The offending program will receive a TERMINATE signal from procmail, and processing of the rcfile will continue. If zero, then no timeout will be used and procmail will wait forever until the child has terminated; if not specified, it defaults to 960 seconds.

- man procmailex 有很多範例

```
:0*             # 針對所有內容,只要有下面的資訊
^From.*joshua*
^Subject:.*ADSL
{               # 因為一行寫不完，所以用 {} 刮起來
    :0 c        # 轉寄副本到底下的email
    ! Jim@somedomain.org

    :0:         # 將信件放到 ADSL 檔案中
    ADSL
}

#將某人的來信移到 $MAILDIR/trash 檔案中
:0
* ^.*From.*someone@somewhere.com
trash

#主旨含有 meeting 字串的信另存一份到 $MAILDIR/meeting 檔案中
:0 c
* ^Subject:.*meeting
meeting

#將來自 yahoo.com.tw 的郵件轉寄副本給 someone
:0 c
* ^From.*@yahoo.com.tw
! someone@somewhere.com

#備份所有郵件到 $MAILDIR/backup 檔案
:0 c
backup

#刪除長度大於 1024768 bytes 的信件
:0
```

```
:0
* > 1024768
/dev/null
```

- 正規表示式驗證 http://osteele.com/tools/rework/
- man pages: procmailex, procmailrc, procmail
- OLS3老師寫得過濾規則 ftp://ftp.tnc.edu.tw/Sysop/MAIL/procmailrc
- 交大的文件 http://www.csie.nctu.edu.tw/~smchen/procmail.htm
- 配合spamassassin 的 procmailrc http://spamassassin.apache.org/full/3.0.x/dist/procmailrc.example

- 專業的判斷spam軟體 http://spamassassin.apache.org/ 可以搭配使用

LAB-Procmailrc:設定procmailrc處理接收到的信件

- 將來自某網域的信件全部備份到某個信箱一份
- 設定 postfix 啟動 procmailrc

```
# vim /etc/postfix/main.cf
ailbox_command = /usr/bin/procmail
# /etc/init.d/postfix restart
```

- 鑽寫針對個人使用者的規則，規則內容為：

```
[mtchang@linux ~]$ more .procmailrc
# 紀錄檔在本地端使用者的 .procmail_log
LOGFILE=$HOME/.procmail_log
# 從 @cm.nnsysu.edu.tw 寄來的信件,複製一份到 mtchang.tw.AT.gmail.com位址
:0 c
* ^From.*@cm.nsysu.edu.tw
! mtchang.tw.AT.gmail.com
```

- 從遠端繼信件到此server測試

```
skip..
```

- 觀看 maillog 檔案,是否有作 procmailrc 分信的動作

1. Oct 12 00:28:53 linux postfix/smtpd[13348]: connect from mail.nsysu.edu.tw[140.117.11.4]
2. Oct 12 00:28:53 linux postfix/smtpd[13348]: 660D4295E0F: client=mail.nsysu.edu.tw[140.117.11.4]
3. Oct 12 00:28:53 linux postfix/cleanup[13351]: 660D4295E0F: message-id=<20091012002345.1B16.2C633CDC@cm.nsysu.edu.tw>
4. Oct 12 00:28:53 linux postfix/qmgr[12125]: 660D4295E0F: from=<mtchang@cm.nsysu.edu.tw>, size=820, nrcpt=1 (queue active)
5. Oct 12 00:28:53 linux postfix/smtpd[13348]: disconnect from mail.nsysu.edu.tw[140.117.11.4]
6. Oct 12 00:28:53 linux postfix/pickup[13091]: 73ADA295E11: uid=500 from=<mtchang>
7. Oct 12 00:28:53 linux postfix/cleanup[13351]: 73ADA295E11: message-id=<20091012002345.1B16.2C633CDC@cm.nsysu.edu.tw>
8. Oct 12 00:28:53 linux postfix/local[13352]: 660D4295E0F: to=<mtchang@linux.jangmt.com>, relay=local, delay=0.07, delays=0.01/0.01/0/0.05, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail)
9. Oct 12 00:28:53 linux postfix/qmgr[12125]: 660D4295E0F: removed
10. Oct 12 00:28:53 linux postfix/qmgr[12125]: 73ADA295E11: from=<mtchang@linux.jangmt.com>, size=1015, nrcpt=1 (queue active)
11. Oct 12 00:28:54 linux postfix/smtp[13356]: 73ADA295E11: to=<mtchang.tw@gmail.com>, relay=gmail-smtp-in.l.google.com[209.85.216.96]:25, delay=1.2, delays=0.02/0.01/0.54/0.65, dsn=2.0.0, status=sent (250 2.0.0 OK 1255278254 9si4655156pxi.13)
12. Oct 12 00:28:54 linux postfix/qmgr[12125]: 73ADA295E11: removed

- 收信驗證結果

到我的gmail收信

- procmailrc 很方便，但是請小心使用在email很大的時候常常會造成 cpu loading 飆高。

接收電子郵件

接收電子郵件

接收郵件的通訊協定

- Post Office Protocol

1. All data, including passwords, is passed in cleartext over TCP port 110
2. Use POP3s to provide SSL encryption of data over TCP port 995

- Internet Mail Access Protocol

1. All data, including passwords, is passed in cleartext over TCP port 143
2. Use IMAPs to provide SSL encryption of data over TCP port 993

- Dovecot supports POP3, POP3s, IMAP, and IMAPs

Service Profile: Dovecot

- Type: SystemV-managed service
- Package: dovecot
- Daemon: /usr/sbin/dovecot
- Script: /etc/init.d/dovecot
- Ports: 110 (pop), 995 (pop3s), 143 (imap), 993 (imaps)
- Configuration: /etc/dovecot.conf
- Related: procmail, fetchmail, openssl

Dovecot Configuration

pop and imap

- pop 及 imap 不加密的設定
- 預設聆聽所有來自 tcp/ip v4 and tcp/ip v6的見面
- 預設的 protocols in /etc/dovecot.conf 開啟你要的通訊服務即可使用

```
#protocols = imap imaps pop3 pop3s
```

- 實際設定及測試

```
[root@station1 etc]# vim /etc/dovecot.conf
# protocols = imap imaps pop3 pop3s # 找到這行改一下
protocols = imap pop3
[root@station1 etc]# /etc/init.d/dovecot restart
正在停止 Dovecot Imap:                                     [失敗]
正在啟動 Dovecot Imap:                                     [  確定
# port 是否有開起， pop 對應 tcp 110 ，imap 對應 tcp 143
[root@station1 ~]# netstat -tulpn | grep dovecot
tcp        0      0 :::110                      :::*
                    LISTEN      622/dovecot
tcp        0      0 :::143                      :::*
                    LISTEN      622/dovecot
# 使用 mutt 收信發信件
[root@station1 ~]# mutt -f pop://student@station1.example.com
[root@station1 ~]# mutt -f imap://student@station1.example.com
```

pops and imaps 加密的設定

- pops and imaps 加密的設定
- 要使用 SSL 加密傳輸需要產生 a private key and self-signed certificate

1. Confirm system time to avoid date issues
2. Review /etc/dovecot.conf for key and cert locations
3. Run make -C /etc/pki/tls/certs dovecot.pem
4. Creates a single PEM file containing both the key and the cert

5. Copy the new PEM file to both locations

- 找到原有系統預設的 key 檔名為 dovecot.pem ，並且將其刪除。

```
[root@server1 certs]# locate dovecot.pem
/etc/pki/dovecot/certs/dovecot.pem
/etc/pki/dovecot/private/dovecot.pem
[root@server1 certs]# pwd
/etc/pki/tls/certs
```

- 使用預設的 Makefile 產生金鑰

```
[root@server1 certs]# make -C /etc/pki/tls/certs dovecot.pem
make: Entering directory `/etc/pki/tls/certs'
umask 77 ; \
        PEM1=`/bin/mktemp /tmp/openssl.XXXXXX` ; \
        PEM2=`/bin/mktemp /tmp/openssl.XXXXXX` ; \
        /usr/bin/openssl req -utf8 -newkey rsa:1024 -keyout $PEM1
-nodes -x509 -days 365 -out $PEM2 -set_serial 0 ; \
        cat $PEM1 >  dovecot.pem ; \
        echo ""    >> dovecot.pem ; \
        cat $PEM2 >> dovecot.pem ; \
        rm -f $PEM1 $PEM2
Generating a 1024 bit RSA private key
.....................................................++++++
.............................++++++
writing new private key to '/tmp/openssl.aD3132'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:TW
State or Province Name (full name) [Berkshire]:station1
Locality Name (eg, city) [Newbury]:taiwan
Organization Name (eg, company) [My Company Ltd]:kaohsiung
Organizational Unit Name (eg, section) []:nsysu
Common Name (eg, your name or your server's hostname) []:cm
Email Address []:root@server1
make: Leaving directory `/etc/pki/tls/certs'
```

- 修改設定檔加入通訊協定及key path

```
[root@server1 certs]# vi /etc/dovecot.conf

protocols = imap pop3 pop3s imaps
#ssl_cert_file = /etc/pki/dovecot/certs/dovecot.pem
#ssl_key_file = /etc/pki/dovecot/private/dovecot.pem
ssl_cert_file = /etc/pki/tls/certs/dovecot.pem
ssl_key_file = /etc/pki/tls/certs/dovecot.pem
[root@server1 certs]# service dovecot restart
Stopping Dovecot Imap:                                     [  OK  ]
Starting Dovecot Imap:                                     [  OK  ]
```

- use mutt 來做 imaps 及 pops 測試

```
mtchang@ubuntu:~$ mutt -f imaps://student@station1.example.com
mtchang@ubuntu:~$ mutt -f imap://student@station1.example.com
mtchang@ubuntu:~$ mutt -f pops://student@station1.example.com
mtchang@ubuntu:~$ mutt -f pop://student@station1.example.com
```

Verifying POP Operation

- 驗證server端的操作

1. 圖形介面: Thunderbird and Evolution
2. 文字介面: Mutt and Fetchmail
    1. mutt -f pop://user@server[:port]

2. mutt -f pops://user@server[:port]

```
mutt -f pop://mtchang@140.117.79.199
```

- 能夠使用 telnet (POP3) or openssl s_client (POP3s)

1. Identify problems with certificate date or permissions

- 手動驗證 pop3

```
mtchang@ubuntu:~$ telnet 140.117.79.199 110
Trying 140.117.79.199...
Connected to 140.117.79.199.
Escape character is '^]'.
+OK Dovecot ready.
user mtchang
+OK
pass qw
+OK Logged in.
list
+OK 1 messages:
1 611
.
retr 1
+OK 611 octets
Return-Path: <root@localhost.localdomain>
Received: from server1.example.com (localhost.localdomain [127.0.0.1])
        by server1.example.com (8.13.8/8.13.8) with ESMTP id m2P7BxgH002918
        for <mtchang@server1.example.com>; Tue, 25 Mar 2008 15:11:59 +0800
Received: (from root@localhost)
        by server1.example.com (8.13.8/8.13.8/Submit) id m2P7Bw2h002917
        for mtchang; Tue, 25 Mar 2008 15:11:58 +0800
Date: Tue, 25 Mar 2008 15:11:58 +0800
From: root <root@localhost.localdomain>
Message-Id: <200803250711.m2P7Bw2h002917@server1.example.com>
To: mtchang@localhost.localdomain
Subject: test
Lines: 1

test
.
quit
+OK Logging out.
Connection closed by foreign host.
mtchang@ubuntu:~$
```

Verifying IMAP Operation

- Verifying server operation

1. Graphical: Thunderbird and Evolution
2. Text-mode: Mutt and Fetchmail
    1. mutt -f imap://user@server[:port]
    2. mutt -f imaps://user@server[:port]

- Can also use telnet (IMAP) or openssl s_client (IMAPs)

1. Identify problems with certificate date or permissions

參考資料

目標檢核

- Inbound and outbound server configuration
- Mail-related protocols: SMTP, IMAP, POP3
- Preparation for Lab

- Scenario
- Deliverables
- Please ask the instructor for assistance when needed

實作

MTA setup

- 請設定一各 MTA to receive mail ，並且符合下列條件：

1. 能夠允許 relay from 192.168.0.0/24
2. 寄信到使用者 mis@station1.example.com 的信件會被轉寄到 alex,julia
3. 啟動 enable pop server ，並且測試可以載本機及遠端收信

dovecot setup

- 設定 dovecot 可以支援 pop3 和 imap 的 SSL 連線測試，並請使用個 user 作測試

1. dovecot 拒絕 .my123.com domain的連線
2. make -C /etc/pki/tls/certs dovecot.pem 請輸入自己的主機名稱及Email即可。

回到索引頁 or 回到首頁